Exhibit 5

Excerpts of SW-SEC00001497

solarwinds

SECURITY & COMPLIANCE PROGRAM QUARTERLY OVERVIEW

AUGUST 16, 2019

Agenda

Security & Compliance Program

- Security | Compliance Project Highlights
  - Executive Asks
- Introduce Security Score Card
- Security Incident Improvement Plan (SIIP) Update

SolarWinds Security Program

SECURITY CONTROLS BASED ON NIST CONTROLS

Protect

- Next Generation Firewalls / Web Application Firewalls
- Endpoint Protection and Encryption
- Data Leakage Protection
- Spam / Phishing Detection / Response
- Authentication, Authorization and Identity Management

Respond

- Cyber Incident Response Program
- GDPR Operations
- Major Incident Response
- Continuous Improvement

Identify

- Asset Management
- Secure Software Development Lifecycle (SSDL)
- Open Source License Scanning
- Product Certifications (ISO, SOC2)
- NIST internal program assessment
- Vendor Management/Procurement

Detect

- Vendor Data Protection Audits
- Vulnerability Scanning
- Internal / External PEN Testing
- Static / Dynamic Code Analysis
- Open Source Code Inspection

Recover

- Backup
- Disaster Recovery / Business Continuity
- Forensics

SolarWinds Scorecard

NIST Maturity Level

Security Category	2017	2018	2019
Identify	0.8	2.0	3.0
Protect	1.5	3.0	3.2
Detect	1.0	2.8	3.6
Respond	0.8	2.8	3.6
Recover	0.7	2.0	2.0
Overall	1.0	2.5	3.1

Maturity Level	Description
0	There is no evidence of the organization meeting the security control objectives or is unassessed
1	The organization has an ad-hoc, inconsistent, or reactive approach to meeting the security control objectives
2	The organization has a consistent overall approach to meeting the security control objectives, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance
3	The organization has a documented, detailed approach to meeting the security control objectives, and regularly measure its compliance
4	The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations
5	The organization has refined its standards and practices focusing on ways to improve its capabilities in the most efficient and cost effective manner

INDENTIFY

Highlights

- Instituted standardized security scoring method (CVSS). 421 internally discovered issues marked security | 292 resolved in 1H 2019
- Open Source License Scanning coverage across entire portfolio
- Full lifecycle software asset management
- ISO certifications achieved for RMM, Backup, Take Control. N-central, Mail Assure (In progress), SOC 2 Type 1 for Passportal, Loggly & App Optics (in progress)
- Threat intel ingestion remains a manual process

Security Category	Objective	NIST Maturity Level
Asset Management	Internally and externally facing assets are identified and actively managed	**3**
Secure Software Development Lifecycle (SSDL)	Employees are aware of an utilize a security software development lifecycle in their day to day activities	**2**
Open Source License Scanning	Open source code used is scanned and remediated as needed	**3**
Product Certifications	ISO 27001 information security management system (ISMS) framework of policies and procedures are followed and audited annually	**3**
NIST internal program assessment	The internal security program and practices are aligned with NIST	**3**
Vendor Management / Procurement	Vendor management and procurement practices include security reviews for each asset	**5**
	Identify Maturity Level	**3.2**

PROTECT

Highlights

- Access and privilege to critical systems / data is inappropriate. Need to improve internal processes | procedures
- Comprehensive firewall protection for Corporate IT and web properties (Palo Alto Next Gen firewalls in place (58) | Web Application Firewalls (WAF) on all key marketing properties)
- Improved end point protection. End user devices coverage: 80% SEP | 85% encryption | 95% DLP. IT servers coverage: 91% SEP. Hosted environment assessment WIP
- Moving towards Zero Trust model (where we loosely protect all and strongly protect those that can-do material harm). Less requirements on VPN
- Spam / Phishing still a challenge. Adversaries are getting better. Increase in whale phishing (55 million messages blocked 1H2019)
- Movement to make Azure AD authoritative source of identity. Plan to enable federation for all critical assets
- Additional monitoring via SOC is planned for 2nd half of the year

Security Category	Objective	NIST Maturity Level
Next Generation Firewalls	Palo Alto Firewalls are deployed and actively monitored across the company	**5**
Web Application Firewalls	WAFs are deployed for marketing properties but not for production products	**3**
Endpoint Protection and Encryption	Endpoint protection and encryption is deployed and actively managed across the company	**4**
Data Leakage Protection	Data leakage protection is deployed across the company and actively monitored	**3**
Spam / Phishing Detection / Response	Email protections are in place to monitor spam, detect phishing and deter known email scammers	**3**
Authentication, Authorization and Identity Management	User identity, authentication and authorization are in place and actively monitored across the company	**1**
	Protect Maturity Level	**3.2**

DOIT Lead – Rick Holmberg, Kellie Pierce
Business – Enterprise
Executive Sponsor –Rani Johnson

FINANCIAL: ENTERPRISE ACCESS MANAGEMENT (SOX COMPLIANCE)

Description

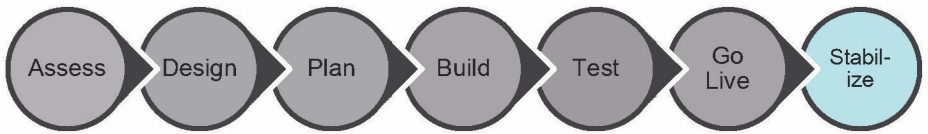
Access management describes the management of individual identities, their authentication, authorization, roles, and privileges within the enterprise in order to minimize security risks associated the use of privileged and non-privileged access.

Scope:

- Enterprise information systems (CoreIT, MSP, Cloud)
- Privileged and non-privileged users
- On-premise & SaaS applications

KPIs

Timeline



Budget

Q1 18	Q2 18	Q3 18	Q4 18	TOTAL
$0	$0	$0	$0	**$0**

Issues, Risks & Dependencies

Cat No.	Description	Action Required
I.1	Concept of least privilege not followed as a best practice	ID existing permission levels within the enterprise
I.2	Use of shared accounts throughout internal and external applications	Work with teams to decommission use of shared accounts
I.3	Project scope expanded to include SOX compliance requirements	Need to assess existing controls to ensure alignment with SOX requirements

Key Milestones / Status

Ph.	Milestone	Start	Finish	Status
1	Align access controls and permissions to security standards and guidelines	1/1/2018	4/20/2018	Complete
2	Map existing assessment of access controls to defined guidelines and standards.	2/1/2018	6/29/2018	Complete
3	Align / validate access controls with SOX compliance requirements. Outline MVP objectives	6/29/2018	7/31/2018	Complete
4	Identify extended team roles and responsibilities	7/1/2018	7/31/2018	Complete
5	Identify admins / approvers, define ABAC	7/1/2018	8/30/2018	Complete
6	Define standards, approval workflows, long term solution/recommendations/POC	8/1/2018	9/30/2018	Complete
7	Finalize Access SARF. Implement SARF changes / exceptions	12/2019	2/2019	Complete
8	Internal audit, Holtzman audit, Audit remediation	1/2019	2/2019	Audit in Progress

InfoSec: DOIT

SECURITY INCIDENT IMPROVEMENT PLAN (SIIP)

Security Focus Area	Action	Owner	Target Timing	July 2019 Status
Process Improvements	Evaluate product, network and system security. • Checkmarx adoption / KPI • JIRA Security Tagging adoption / KPI • Vulnerability Scanning & Reviews with DOIT	T. Brown E. Quitugua K. Pierce	Ongoing	KPI creation: Underway DOIT vulnerability review: Ongoing
	Build Library of authoritative source of practices/processes, agreed to by engineering leadership	K. Pierce	• Q2-2019: List compiled • Q3-2019: Alignment with Engineering	Complete
	Improve Security Practice for the Company (SIIP)	T. Brown E. Quitugua K. Pierce	Ongoing	In Progress
Tools & Technology	Compile cumulative list of security tools and services for the organization (Security Tool Rationalization)	T. Brown E. Quitugua K. Pierce	Q2-2019	Complete
Training	Implement quarterly Incident Response Training	E. Quitugua	Ongoing Q2-Complete Q3- 8/19/19 Q4-TBD	In Progress
	Continue GDPR Bootcamp training. Refresh training materials	K. Pierce	Ongoing	Ongoing